5

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/647,644	08/25/2003	Mark Eric Obrecht	6002-00602	2528

7590 03/08/2007

B. Noel Kivlin
Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	**PAPER NUMBER**
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/647,644	**Applicant(s)** OBRECHT ET AL.	
	Examiner Arezoo Sherkat	**Art Unit** 2131	\

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/11/2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *105-128* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Response to Amendment

This office action is responsive to Applicant's amendment received on 12/11/2006. Claims 1-104 have been cancelled. Claims 105-128 have been added. Claims 105-128 are pending.

Response to Arguments

Applicant's arguments with respect to claims 105-128 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims105-128 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balasubramaniam et al., (U.S. Patent No. 6,671,812 and Balasubramaniam hereinafter), in view of Muttik, (U.S. Patent No. 6,775,780).

Regarding claim 105, Balasubramaniam discloses a computer-implemented method comprising:

selecting an active program on a computer system as code under investigation, wherein at least some of the code associated with the selected active program is running in kernel mode (i.e., searching for and deleting unused, obsolete, unneeded, or undesired software, components, or data on the user computer)(col. 14, lines 4-18), and executing malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a plurality of detection routines (i.e., anti-virus program), wherein said executing includes: applying the plurality of detection routines to the code under investigation, wherein said applying includes associating weights to the code under investigation in response to detections of a valid program or malicious code; and determining whether the code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines (i.e., performing a software and hardware diagnositcs on the user computer and providing a health report card for the user computer)(col. 10, lines 20-67 and col. 11, lines 1-10).

Moreover, Muttik discloses the detection routines are applied to a given code to associate weights to the code in response to detection of a valid or malicious piece of code (fig. 2, item 212 - col. 5, lines 14-36).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Balasubramaniam with teachings of Muttik because it would allow to include associating possitive and negative weights for suspicious and non-malicious activity as disclosed by Muttik. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Muttik to keep a count of the total weight which is compared against a threshold value (Muttik, col. 5, lines 14-20).

Regarding claims 115, 127, and 128, Balasubramaniam discloses a computer-implemented method comprising:

selecting a program currently running on a computer system as code under investigation, wherein said program is running in a manner that permits infection of said computer system (i.e., searching for and deleting unused, obsolete, unneeded, or undesired software, components, or data on the user computer), and executing malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a plurality of detection routines (i.e., anti-virus program), wherein said executing includes: applying the plurality of detection routines to the code under investigation, wherein said applying includes associating weights to the code under investigation in response to detections of a valid program or malicious code, and determining whether the code under investigation is a valid program or malicious code [as a function of the weights associated by the detection routines](i.e., performing a software and hardware diagnositcs on the user computer and providing a health report card for the user computer)(col. 10, lines 20-67 and col. 11, lines 1-10).

Moreover, Muttik discloses the detection routines are applied to a given code to associate weights to the code in response to detection of a valid or malicious piece of code (fig. 2, item 212 - col. 5, lines 14-36).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Balasubramaniam with teachings of Muttik because it would allow to include associating possitive and negative weights for suspicious and non-malicious activity as disclosed by Muttik. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Muttik to keep a count of the total weight which is compared against a threshold value (Muttik, col. 5, lines 14-20).

Regarding claims 106 and 116, Balasubramaniam discloses the method of claim 105, wherein the code under investigation has access to other active programs executing on the computer system (i.e., a virus or malicious code on the computer system damages the computer system because it has access to other active programs executing on the computer system)(col. 10, lines 44-62 and col. 14, lines 4-18).

Regarding claims 107 and 118, Balasubramaniam discloses the method of claim 105, further comprising:

selecting one or more additional active programs as code under investigation, and executing said MCDC with respect to said code under investigation (col. 10, lines 44-62).

Regarding claims 108 and 119, Balasubramaniam discloses the method of claim 105, wherein the plurality of detection routines includes a plurality of valid program detection routines and a plurality of malicious code detection routines, wherein each of the plurality of detection routines individually associates weights to the code under investigation in response to detections of a valid program or malicious code (i.e., performing a software and hardware diagnositcs on the user computer and providing a health report card for the user computer)(col. 10, lines 20-67 and col. 11, lines 1-10).

Moreover, Muttik discloses the detection routines are applied to a given code to associate weights to the code in response to detection of a valid or malicious piece of code (fig. 2, item 212 - col. 5, lines 14-36).

Regarding claims 109-114 and 120-126, Balasubramaniam discloses the method of claim 105, wherein the malicious code includes remote control software, a keystroke logger, spyware, a worm, a Trojan horse, and monitoring software (i.e., viruses and unused, obsolete, unneeded, or undesired software, components, or data on the user computer)(col. 10, lines 44-64).

Regarding claim 117, Balasubramaniam discloses the method of claim 115, wherein at least some of the code associated with the selected active program is running in kernel mode (col. 14, lines 4-18 and col. 10, lines 44-63).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

A.S.
Patent Examiner
Group 2131
March 1, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100